Information Security Primer

Helping the Energy Industry adapt to the Internet Age, without compromising operational security or operating flexibility

Prepared for EPRI
by
Secure Computing Corporation
George D. Jelatis,
Principal Investigator

EPRI Project Manager,
Joe Weiss

Executive Overview

Information is a critical business resource for nearly every modern industry. Communication of critical business information and controlled sharing of that information are essential parts of all business operations and processes. Modern networking technologies, such as the Internet, offer new tools for making the communication and sharing of information more efficient, and faster than ever before. Networking, however, can significantly increase the enterprise's business risk, through increased exposure to information security risks.

Presidential Decision Directive (PDD63) has specifically identified the electric and energy industries as part of the nation's critical infrastructure. It is expected that the EPRI Enterprise Infrastructure Security (EIS) Program and this Primer can help meet the intent of the Directive. As the deregulation of the energy industry unfolds, information security will become more important. For the energy-related industries, the need to balance the apparently mutually exclusive goals of operating system flexibility with the need for security will need to be addressed from a business perspective. Consequently, the intent of this Primer is to provide a current status of electronic security technology, educate energy industry senior executives and other non-IT personnel on information security issues, and explain how these issues can affect the energy industry.

This Primer provides information on basic electronic security principles. It applies these principles to the utility industry in order to show why information security is critical. It is expected that this Primer will be a first volume of a series of guidelines that the industry will produce to help meet the challenge of electronic infrastructure security.

Acknowledgements

The authors want to acknowledge the contribution of Bruce Gillham of EPRI's Gateway Team and Terry Shidla of Secure Computing Corporation for helping make this Primer available on such short timeframe.

Copyright information

Table of Contents

Introduction

Information is a critical business resource for nearly every modern industry. Communication of critical business information and controlled sharing of that information are essential parts of all business operations and processes. Modern networking technologies, such as the Internet, offer new tools for making the communication and sharing of information more efficient and faster than ever before. Networking, however, can significantly increase the enterprise's business risk, through increased exposure to information security risks.

Several points also need to be considered:

- To date, most threats originate from inside an organization.
- Not all threat agents are necessarily malicious. Some threats can be unintentional, but no less destructive.
- Vulnerabilities can also be due to poor people processes, policies, maintenance processes, technologies, systems, interfaces, etc.

In October of 1997, the President's Commission on Critical Infrastructure Protection published a report that called for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures. Presidential Decision Directive (PDD63) builds on the report recommendations and documents the President's policy on the identified issues. Specifically, PDD63:

- Sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003,
- Requires the Federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained;
- Seeks the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships;
- Protects privacy rights and seeks to utilize market forces. It is meant to strengthen and protect the nation's economic power, not to stifle it.

PDD63 has specifically identified the electric and energy industries as part of the nation's critical infrastructure. It is expected that the EPRI Enterprise Infrastructure Security (EIS) Program and this Primer can help meet the intent of the Directive. (Additional information on PDD63 and EIS can be obtained from EPRI.)

As the deregulation of the energy industry unfolds, information security will become more important. For the energy-related industries, the need to balance the apparently mutually exclusive goals of operating system flexibility with the need for security will need to be addressed from a business perspective. Then consequently the intent of the Primer is to:

- provide a current status of electronic security technology,
- educate energy industry senior executives and other non-IT personnel on information security issues, and

- explain how these issues can affect the energy industry.

The Primer provides information on basic electronic security principles. It applies these principles to the utility industry in order to show why information security is critical.

Energy Industry Control & Information Management Systems

1. Electrical Power Systems and Operation[1,2]

Key electric energy operational systems depend on real-time communication links both internal and external to the enterprise. The functional diversity of these organizations has resulted in a need for these key systems to be designed with a focus on open systems that are user configurable to enable integration with other systems both internal and external to the enterprise. In many cases, these systems can be reconfigured using telecommunication technologies and in nearly all cases the systems dynamically exchange data in real time. This results in a need for highly reliable, secure control and information management systems.

1.1. Energy Management System (EMS)

The objective of the EMS is to manage the production, purchase, transmission, distribution and sale of electrical energy in the power system at a minimal cost with due respect to safety and reliability. Management of the real-time operation of an electric power system is a complex task requiring the interaction of human operators, computer systems, communications networks, and real-time data-gathering devices in power plants and substations.

An EMS consists of computers, display devices, software, communication channels and remote terminal units that are connected to Remote Terminal Units (RTUs), control actuators, and transducers in power plants and substations. The main tasks it performs have to do with generator control and scheduling, network analysis and operator training. Control of generation requires that the EMS maintain system frequency and tie line flows while economically dispatching each generating unit. Management of the transmission network requires that the EMS monitor up to thousands of telemetered values, estimate the electrical state of the network and to inform the operator of the best strategy to handle potential outages that could result in an overload or voltage limit violation. EMS's can have real time two way communication links between substations, power plants, independent system operators, and other utility EMS's.

1.2. Supervisory Control and Data Acquisition (SCADA) System

A SCADA system supports operator control of remote (or local) equipment, such as opening or closing a breaker. A SCADA system provides three critical functions in the operation of an electric power system:

- Data acquisition

[1] Standard Handbook for Electrical Engineers, Thirteenth Edition, McGraw-Hill, Inc.
[2] The Electrical Engineering Handbook, Second Edition, CRC Press & IEEE Press

- Supervisory control
- Alarm display and control

It consists of one or more computers with appropriate applications software connected by a communications system to a number of RTUs placed a various locations to collect data, to perform intelligent control of electrical system devices and to report results back to an EMS.

SCADAs can also be used for similar applications in natural gas pipeline transmission and distribution applications.

A SCADA can have real time communication links with one or EMSs and hundreds of substations.

1.3. Remote Terminal Unit (RTU)

RTUs are special purpose microprocessor-based computers which contain analog to digital converters (ADC) and digital to analog converters (DAC), digital inputs for status and digital output for control. There are transmission substation RTUs and distribution automation (DA) RTUs. Transmission substation RTUs are deployed at substation and generation facilities where a large number of status and control points are required. DA RTUs are used to control air switches and var compensation capacitor banks on utility poles, to control pad-mounted switches, to monitor and automate feeders, to monitor and control underground networks and for various uses in smaller distribution substations. RTUs are also used in natural gas transmission and distribution in a similar manner. RTUs can be configured and interrogated using telecommunication technologies. They can have hundreds of real time communication links with other substations, EMS, and power plants.

1.4. Programmable Logic Controller (PLC)

PLCs have been used extensively in manufacturing and process industries for many years and are now being used to implement relay and control systems in substations. PLCs have extended I/O systems similar to transmission substation RTUs. The control outputs can be controlled by software residing in the PLC as well as via remote commands from a SCADA system. The PLC user can make changes in the software stored in EEPROM without making any major hardware or software changes. In some applications, PLCs with RTU reporting capability may have advantages over conventional RTUs. PLCs are also used in many power plant and refinery applications. They were originally designed for use in discrete applications such as coal handling. They are now also being used in continuous control applications such as feedwater control. PLCs can have many real time communication links inside and outside the substation or plants.

1.5. Protective Relays

Protective relays are designed to respond to system faults such as short circuits. When faults occur, the relays must signal the appropriate circuit breakers to trip and isolate the faulted equipment. Distribution system relaying must coordinate with fuses and reclosures for faults while ignoring cold-load pickup, capacitor bank switching and transformer energization. Transmission line relaying must locate and isolate a fault with sufficient speed to preserve stability, to reduce fault damage and to minimize the impact on the power system. Certain types of “smart” protective relays can be configured and interrogated using telecommunication technologies.

1.6. Automated Metering

Automated metering is designed to upload residential and/or commercial gas and/or electric meter data. This data can then be automatically downloaded to a PC or other device and

transmitted to a central collection point. With this technology, real time communication links exist outside the utility infrastructure.

1.7. Plant Distributed Control Systems (DCSs)

Plant Distributed Control Systems are plant-wide control systems that can be used for control and/or data acquisition. The input/output (I/O) count can be as high as 20,000 data points or higher. Often, the DCS is used as the plant data highway for communication to/from intelligent field devices, other control systems such as PLCs, RTUs, and even the corporate data network for Enterprise Resource Planning (ERP) applications. The DCS traditionally has used a proprietary operating system. Newer versions are moving toward open systems such as Windows NT, Sun Solaris, etc. DCS technology has been developed with operating efficiency and user configurability as drivers, rather than system security. Additionally, technologies have been developed that allow remote access, usually via PC, to view and potentially reconfigure the operating parameters.

1.8. Field Devices

Examples of field devices are process instrumentation such as pressure and temperature sensor and chemical analyzers. Other standard types of field devices include electric actuators. Intelligent field devices include electronics to enable field configuration, upload of calibration data, etc. These devices can be configured off-line. They also can have real time communication links between plant control systems, maintenance management systems, stand-alone PCs, and other devices inside and outside the facility.

1.9 Telecommunications Links

SCADA and EMS system operations are critically dependent on the telecommunication links which gather data from geographically dispersed sources and transmit operational and control instructions to geographically dispersed facilities. In the North American grid these telecommunications links run the gamut from hardwired private networks to multi-network systems using a combination of private and public networks for both data acquisition and control. Not all of the networks are hardwired. Microwave and satellite communications links are common alternatives in areas were the topography and/or distance makes wireless more cost effective. At first glance it would seem that a private, hardwired network which is totally within the control of the owner organization is a secure system. However even the hardwired private networks will be linked to networks outside the control of the company. Typical outside data sources are bulk power customers, major retail customers, bulk power providers, power pools, independent system operating entities, etc. These connections can offer a multitude of paths into the SCADA and EMS systems. Without proper security design and management, each of these links is a potential security risk.

Power plant DCS systems produce information which are necessary for dispatch and control. This requires real-time information flow between the power plant and the utility's control center, the system dispatch center, regulatory authorities, etc. A power plant operating as part of a large wholesale power network may have links to an independent system operator, a power pool, etc. Thus as the generation business moves more and more into market-driven competitive operation, both data integrity and confidentiality will become major concerns for the operating organizations.

Any telecommunication link which is even partially outside the control of the organization owning and operating power plants, SCADA systems or EMS's represents a potentially insecure pathway into the business operations of the company as well as a threat to the grid itself. The interdependency analyses done by most companies during Y2K preparations has both identified these links and the systems vulnerability to their failures. Thus they provide an excellent reference point for a cyber-vulnerability analysis.

2. Integrated Utility Network

The energy industry has historically operated closed, tightly controlled networks. Deregulation and the resulting commercial influences have placed new information sharing demands on the energy industry. Traditional external entities like suppliers, consumers, regulators and even competitors now must have access to segments of the network. The definition of the network must be expanded to include the external wide area network connections for these external entities. This greatly increases the security risk to other functional segments of the internal network that must continue to be protected from these external connections. This is true whether a private network or the Internet is used to support the external wide area network.

The external entities already have connections to the Internet and as such the Internet can provide the backbone for the External Wide Area Network. Duplicating this backbone to create a private network requires not only large up front start up costs, but also ongoing maintenance costs and potentially higher individual transaction costs than using the Internet.

The diagrams of the Utility Communications Architecture (UCA™) illustrate the traditional internal network segments and the connections to External Wide Area Networks. These diagrams can be obtained by request through EPRI. This is being done in an effort to limit the size of this primer document to facilitate electronic distribution.

Security Overview

3. Information Security

The electric power industry traditionally has been a vertically integrated industry that operated in pseudo-monopolistic fashion. However, the industry is currently undergoing a restructuring, which in many cases, is resulting in a break-up of the vertical structure. Additionally, there has been a significant move on the part of the control system suppliers to the electric and petrochemical industries toward open, user-configurable systems utilizing real time communications. With a vertical structure, local and wide-area networks were sufficient to maintain a reasonably secure data network. However, deregulation and new networking technologies are making secure communications more important and also more difficult to develop and maintain.

Information security is essentially concerned with the relationships between people and information. In these relationships, people are the owners, custodians, creators, readers, modifiers, certifiers, or even subjects of the information. It follows then that the information itself is the object of various actions by people — creation, destruction, reading, modification, certification. Information security is concerned with first defining the appropriate relationships between people as actors and information resources as objects; these relationships are usually defined as a set of rules defining permitted actions. It should be noted that not all threats come from outside the organization nor are all threats malicious in nature.

Information security is, then, concerned with controlling the relationships between people and information so that information is managed according to well-defined rules. Some human agent or institutional agency of authority is usually charged with creating, communicating, applying, monitoring and enforcing these information security rules. Some examples or models of contemporary information security rules are:

- rules for handling of government classified documents;
- rules for ensuring client-attorney privilege or the privacy of shared information;
- rules followed by corporate accountants and checked by financial auditors; and
- rules for ensuring the accuracy and completeness of patients' health records.

Generally these rules define information security controls that are based on the information security properties of special classes of information; these properties fall into three broad categories:

- **confidentiality** of sensitive information;
- **integrity** and **authenticity** of critical information; and
- **availability** of necessary information.

In order to apply these rules we need to be able to identify the categories or properties of the information, as well as the identities of every person who seeks to use that information. In the "pen and paper" or social world,

- people attach **labels to documents** containing information, or define "classification rules" by which a reasonable person may **decide on a document's classification**;
- people can **evaluate a document's authenticity** based on its source or on its physical properties such as a signature or notary's seal;
- people can usually **evaluate a document's integrity** because they can detect when a document has been modified by the physical traces the modification inevitably leaves on the physical document; and
- people **identify other people reliably** by name, handwriting, face or voice, if we know them personally; and by **credentials** such as a driver's license, passport or personal reference, if we have never met them face-to-face.

When information moves into the computer system or information technology domain, the information security rules often stay the same, but the means available for enforcing them must be far simpler than in a social context. The rules must be simpler because computer systems, as agents of information security control have several major limitations when compared with people:

- while a computer can deal with **labels**, the computer system is incapable (for the present) of **applying rules based on the semantic content** or meaning of information in order to **decide on a document's classification**;
- the computer cannot **evaluate a document's authenticity or integrity** based on the electronic document itself, because when information moves into the information technology domain, it loses its representational binding to a physical medium; and
- the computer system cannot distinguish one person from another as easily or surely as humans do, so it **cannot identify people reliably** unless the person presents some **computer readable credential**.

Information security for information technology faces, then, three challenges:

- defining an appropriate, applicable security model;
- deriving information control rules based on that model; and
- implementing control mechanisms that apply those rules, consistently, and without fail.

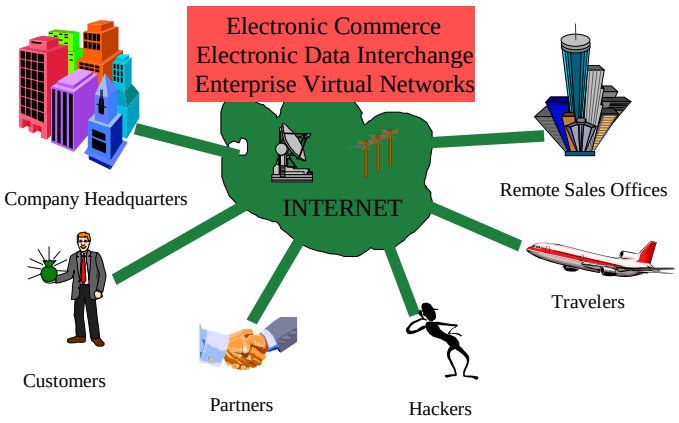
4. The Internet and Intranets

4.1. The Internet: a Network of Networks

The Internet is a "network of networks". The Internet is based upon the TCP/IP (Transmission Control Protocol & Internet Protocol) communication protocol standards for communication between networks. Any network that uses TCP/IP can "participate" in the Internet. The Internet was conceived to promote sharing of data efficiently over expensive physical links with limited bandwidth. The emphasis on sharing and efficiency, along with the relatively closed community in which these advantages were developed, led to a complete

absence of security measures in the Internet protocols. The Internet is convenient, efficient, extremely effective, and fundamentally insecure.

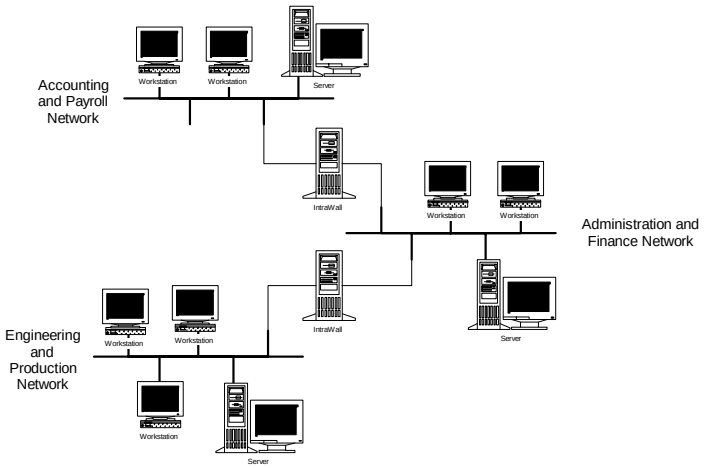
The Internet is an attractive resource because of the large community of users, and because of the large quantity of information available on its tens of thousands of connected host computers. While electronic mail (e-mail) and file transfer exchanges to and from remote hosts have long been attractive features of the Internet, the recent development of the "World Wide Web" protocols, servers, and browsers has led to exponential growth in its use and utility.



An enterprise network with no IP-level connections to the outside world is a "stand-alone" network, separate from the Internet. It is also a network that, while completely secure against outside threats, is of rather limited utility. Thus, while connection to the Internet brings clear benefits, it must be done carefully so as not to bring unacceptable risks as well.

4.2. Intranets

An "intranet" is an intra[mural] network of networks. More and more enterprises are finding that Internet technology can be used to integrate and inter-connect their internal networks to provide improved communication and controlled sharing of information.



Intranets, thus, usually use the same protocols and technology as the Internet—TCP/IP, SMTP, HTTP, etc.— to allow users on one internal network (often a local area network or LAN) to communicate with users on another network. Besides the replacement of memos and phone calls with e-mail, many enterprises have begun to maintain internal "websites" holding libraries of corporate information such as Policy and Procedure Manuals, Quality Manuals, corporate mission statements, employee phone lists, etc.

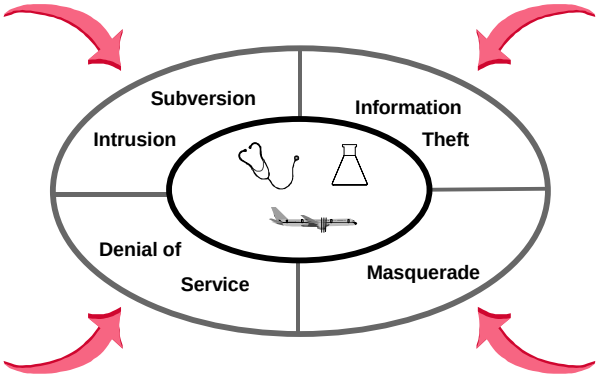
Corporate intranets are likely to connect networks with restricted information, such as "human resources" or "corporate planning", with others having a very broad community of authorized users, such as "engineering" or "production". In such cases, it may be necessary to control the flow of information across the boundaries between these various internal networks, just as it would be necessary to control the flow of information between internal networks and the Internet.

Thus intranets present a control problem that, while generally presenting much lower risk than the Internet, is analogous to the Internet problem and may be just as important.

5. Risks, Threats and Vulnerabilities

5.1. Internet Business Related Risks

Connection to the Internet can create risks that affect the ability to meet business objectives. These business risks include financial loss and/or other commercial harm. Assessing and quantifying these risks is difficult and complicated, and depends upon the value of enterprise information, the external and internal threats, and the internal system vulnerabilities.



There are four broad categories of information security risks:

- Information theft
- Intrusion and subversion of system resources
- Masquerade
- Denial of service

Each of these information security risks can lead to business risks. All of these information security risks are greatly magnified by connection to the Internet. Connection to the Internet not only provides people within the enterprise access to the rest of the Internet, but the same connection can effectively make the enterprise network a part of the Internet, and thus accessible by all of the millions of users of the Internet. Even though many critical energy industry processes and data currently do not utilize the Internet, the Internet's reduced cost structure will eventually make its use more commonplace.

5.2. Information Security Risks

Basically, an InfoSec risk is the possibility that a "threat agent" or attacker will succeed in exploiting a system vulnerability. Normally we are only concerned about those InfoSec risks that lead to some consequent loss to the enterprise attacked.

An InfoSec threat can be defined as an active agent that is part of your operating environment and that seeks to violate or circumvent your information security policy. An assessment of threats is inherently subjective and speculative because it deals with potential threat agents and their possible capabilities.

An InfoSec vulnerability can be defined as an exploitable flaw ("bug") or side effect ("feature") that is in or a part of your information processing systems. An analysis of vulnerabilities can be objective because it deals with properties of your systems. It will, however, always be incomplete because of the practical complexities and scale of the task.

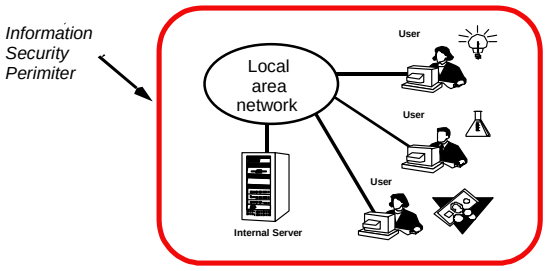
6. Applicable Security Safeguards

6.1. Technical Safeguards

Technical safeguards provide means to identify users and control their access to information systems resources.

6.1.1. Technical Perimeter Controls

Control of connections between an internal network and the Internet requires that we begin by defining a boundary. This boundary, or "information security perimeter", defines the limits within which the enterprise controls all information systems and networks, and outside of which the enterprise has little or no control.

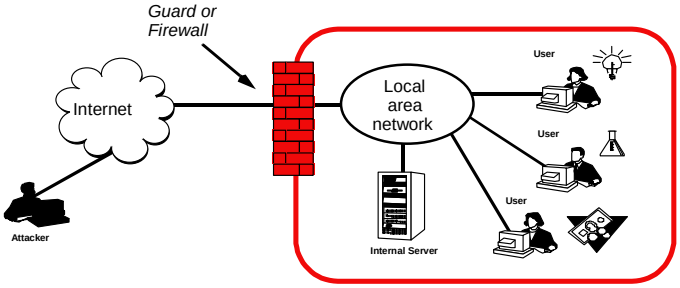


An information security perimeter is the networking counterpart of the physical perimeter that most organizations put in place to protect their internal assets—physical, financial, personnel or information. Like the physical perimeter, the information security perimeter should have a limited number of portals or gateways open to the outside world. Each of these information gateways could exercise the following controls:

- identify everyone who requests access to the site from outside;
- identify everyone who requests access to the outside from within the site;
- enforce restrictions on data flowing into the site;
- enforce restrictions on data flowing out of the site;
- protect the integrity of hosts accessing external systems; and
- conceal the structure and nature of the information systems and networks within the site.

6.1.1.1. Firewalls as Gatekeepers

The computer system that acts as a network gatekeeper, **controlling network traffic that crosses the information security perimeter**, is generally referred to as a "firewall" or "guard"; a firewall because firewalls keep fires from spreading and a guard for obvious reasons.



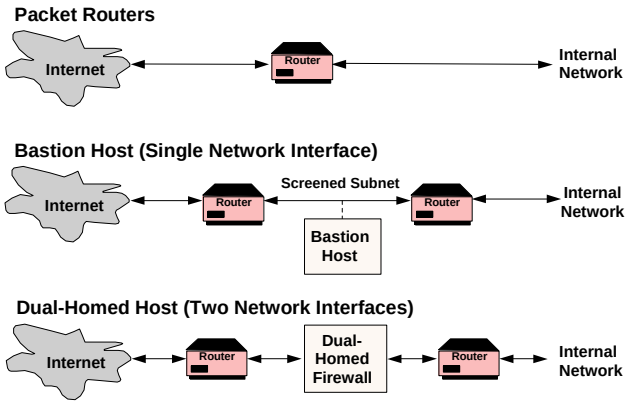
A firewall system resides on the security perimeter or boundary with connections to both internal and external networks. It serves as a network portal or gateway and it can act as a "choke point" though which all boundary-crossing must take place.

6.1.1.2. Typical Firewall Architectures

A network firewall always has two physical network connections: one to the organization's internal networks; and a second to the Internet. The firewall itself is designed for configuration and operation in one of several firewall architectures. We will discuss only the three architectures illustrated here, as they are the most common.

The simplest firewall architecture is an IP protocol router connected between the internal networks and the Internet. This architecture is straightforward to implement because one need only connect a commercial router to the two networks and configure the router. The firewall capabilities of this architecture are quite limited.

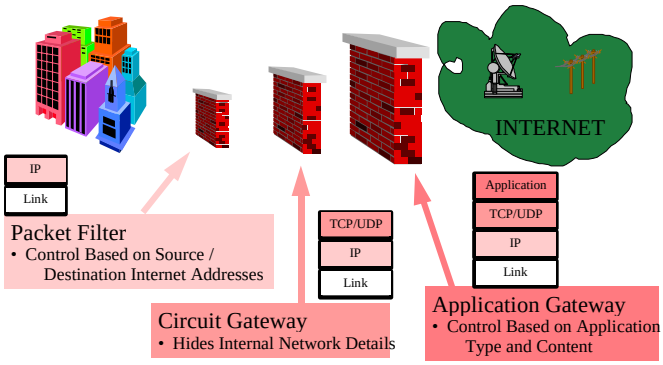
The "screened subnet" architecture is intermediate in complexity and in capabilities. This architecture places a "bastion host" on a subnet that is isolated or "screened" by two routers. This architecture relies on router configuration tables to "force" all traffic to pass through the bastion host.



The "dual-homed" host architecture places the firewall host directly in the path of all traffic between two routers so the firewall cannot under any circumstances be bypassed. This architecture is the most complicated to configure and administer, but it provides the best firewall capabilities.

6.1.1.3. Firewall Effectiveness

While the firewall's placement on the boundary affords it the opportunity to control all cross-boundary data flows, its "effectiveness" will determine how well it exercises this control. For a firewall, we can define effectiveness as the likelihood that the firewall will succeed in enforcing the organizational security policy with respect to cross-boundary data flows and accesses. Stated somewhat differently, a firewall's effectiveness can be measured by how well it blocks all prohibited traffic, while passing all allowed traffic.



Generally, the more information the firewall has about the data it passes, the more effective it can be. However, it should be noted that the more detailed the data evaluation, the greater the system performance penalty.

Computer network protocols are often described in terms of a "stack" of protocols, each layer providing services to the layer above, and using the services of the (generally more primitive) layer below. The firewall can act on network traffic by interposing itself at any one of the protocol layers. Higher layer protocols provide more information about the intent and content of the data they carry, thus the higher the layer at which the firewall operates, the more information it has and the more effective it can be.

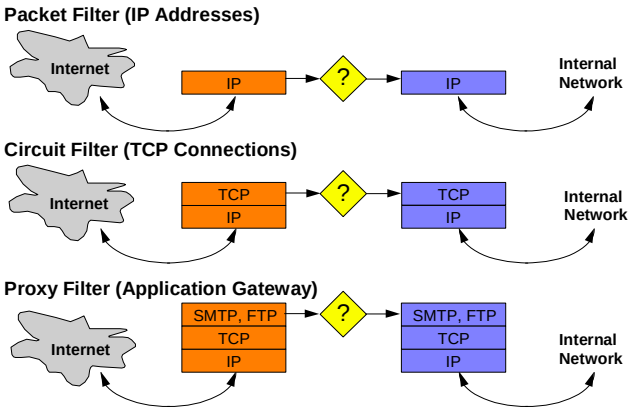
The effects of a firewall acting at each of these different protocol levels is discussed further below.

6.1.1.4. Firewall "Filtering" Approaches

As we have seen, one of the main functions of a firewall is to control the flow of data across the boundary between the protected network and the Internet. The firewall accomplishes this control by examining the "payloads" of the communication protocols, and making a "go/no-go" decision on each one. This is commonly referred to as "filtering" because "good" protocol payloads pass through, and "bad" payloads are blocked.

Today, there are three basic filtering approaches used by firewall systems to control the flow of data:

- Packet Filtering operates on IP-datagrams or "packets". It passes or blocks each packet based upon its source and destination IP-addresses (host addresses), and possibly the type of protocol traffic it carries. Routers often do simple IP-address filtering. At this level there is almost no traffic context or protocol state[3] information available on which to base a filtering decision.



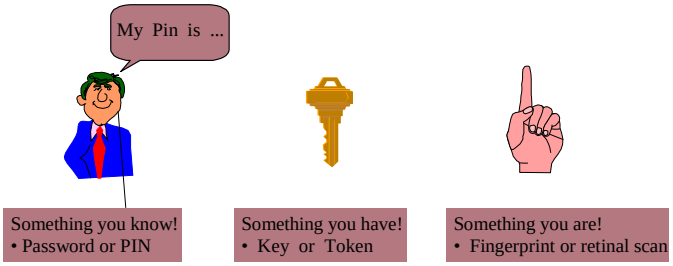
- Circuit Filtering operates on TCP-segments. It allows or blocks transport level connections between client and server processes. These connections or "circuits" are allowed or blocked based on the processes that use them. At this level there is some context information available, but still only a little state information on which to base a filtering decision.

- Application-Level Gateways use proxies that operate on applications protocol messages. The applications proxies can allow or block the passage of these messages based upon the sending process or user, the destination process or user, or even the format or the content of the message. At this level, the proxy has as much state, context, and semantic information as a computer system can have about the end-to-end message traffic. The limitations on filter decisions at this level are computational and theoretic.

6.1.2. Identification and Authentication of Users

All security controls rely on some form of identification of the users of the system. This is generally based on the notion that access or authority entails responsibility, and it is not possible to hold individual persons responsible for their actions if they cannot be unambiguously and certainly identified.

Identification has, in the past, been as "weak" or vague as the understanding that only a limited set of authorized users has access to terminals and computer systems. Today, there is a trend toward the other extreme, where the system may require strong or certain identification of each individual user — identification that is strong enough to be used as evidence in a court of law. There needs to be an understanding for when each level of identification and authentication is necessary.



The three classic means of proving or

[3] The Internet Protocol was designed to operate on each packet without needing any information about packets or events that preceded it. This was a deliberate design decision which relieved the IP protocol implementation of the need to maintain any history information as part of its operating state.

authenticating a user's identity, in order of increasing "strength", are for the user to present as proof of identity:

- something the user **knows**,
  for example, a combination or password;
- something the user **has**,
  for example, a key or cryptographic token; and
- something the user **is**,
  for example, a finger-print, retinal image, or "voice-print".

These authentication proofs are listed in order of increasing strength. Combining two or more of these proofs significantly increases the certainty of the authenticity of a user's identity.

6.1.3. Cryptography

Cryptography is the study and application of codes and ciphers. Its basic tools are encryption and decryption methods, and key management techniques. Encryption methods transform data, using an encryption key, into a form that is not directly usable by people or programs. Decryption methods transform encrypted data, using a decryption-key, back into their original, useful form. Some methods use a single encryption/decryption key, and others use two distinct keys for these two transformations. For example, DES, the US Government's Data Encryption Standard, uses the same key for both encryption and decryption; it is thus called a "symmetric cipher". RSA, named for its inventors, Rivest, Shamir and Adelman, uses one key for encryption and a second, complementary key for decryption; it is, thus, called an "asymmetric cipher". RSA is also referred to as a "public key" cipher because one key can be made public and the other kept secret for use as a digital signature[4].

For this discussion we are really only concerned with the ways in which cryptography can be used to implement a security policy, so the reader is referred to one of the many good references on cryptography, one of the best of which is listed at the end of this paper. It should be noted that these and other cryptographic technologies were either developed or adapted for e-commerce applications. It is not clear that they are as applicable for the highly reliable, and dynamically changing demands of e-operations.

6.1.3.1. Uses of Cryptography

Cryptography can be used to convey private or critical data between correspondents over an uncontrolled, untrustworthy network, such as the Internet. In doing this, it can ensure any one, or all three of the following properties of the data:

- Content Confidentiality
  - application level encryption
    e.g., encrypted messages
  - encrypted communications channel
    e.g., IP encryption or virtual private networks (VPNs)
- Data Integrity
  - cryptographic "check-sums"
    e.g., message digests, hashes
- Authenticity and Non-repudiation

[4] The term "digital signature" is used to refer to the cryptographic equivalent, for an electronic document, of a hand-written signature on a paper document. The digital signature itself is a small (a few hundred bits) "signature block" attached to the "signed" electronic document.

- digital signatures and certificates
- digital notary
- assurance of data integrity

Cryptographic techniques can also be used for authentication or proof of identity:

- Authentication of users to systems.
- Authentication of systems to systems.

6.1.3.2. "What is a crypto-key?"

A cryptographic key is just an unguessable number (a bit or digit string) that is used in a cryptographic algorithm to encrypt or decrypt. Typical key sizes are:

- Secret Key: 40, 56 or 128 bits (12, 17 or 39 decimal digits) long
- Public: 512 or 1024 bits (150 to 300 digits) long

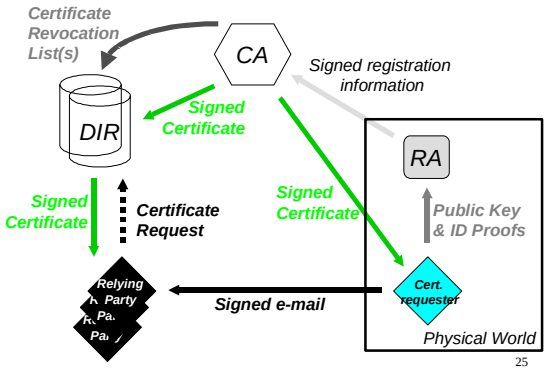
The difficulty or cost of decoding an encrypted message is generally a function of the size of the key (assuming the only useful approach is to try all keys). This decoding difficulty is usually referred to as the strength of the cryptographic key. In 1995 an ad hoc group of cryptographers and computer scientists assembled the following table to illustrate the strength of different key sizes with the Data Encryption Standard (DES) algorithm.

Attacker	*Budget*	*Time to Recover Key*	
		56 bit key	*40 bit key*
Hacker	***$400***	***38 years***	***5 hrs***
Small Bus.	***$10K***	***556 days***	***12 min***
Corp Dept	***$0.3M***	***19 days***	***24 sec***
Big Corp	***$10M***	***13 hrs***	***7 sec***
"XYZ" Agency	***$300M***	***12 sec***	***0.2 milli-sec***

This illustrates rather graphically the importance of key size to data confidentiality. In 1998 the Electronic Frontier Foundation funded the development of a custom-built DES-cracking machine called Deep Crack. Deep Crack was able to decode a 56 bit DES encrypted message in 36–72 hours. Deep Crack cost only $225K, a clear indication that Moore's Law[5] still holds.

6.1.4. PKI Architecture

Digital Certificates are only useful if they are believable (trustworthy) and available when needed. Public Key Infrastructure (PKI) is the term used to describe the organizational and technical infrastructure needed to support the generation, distribution, look-up, and revocation of public key digital certificates.



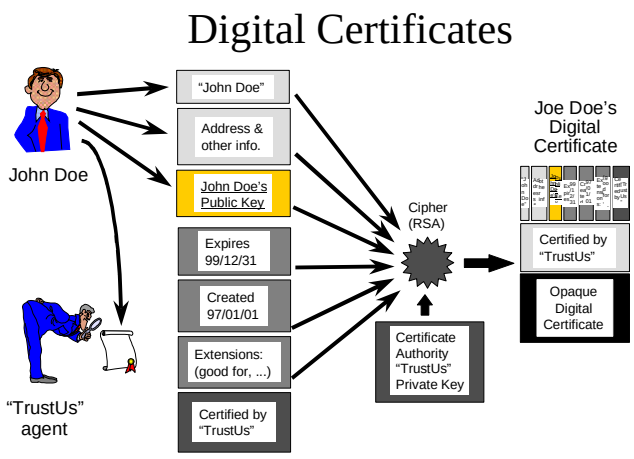
The architecture of a public key infrastructure (PKI) is illustrated in the

[5] Moore's law states that computer hardware performance doubles every eighteen months.

figure to the right. It includes a Certificate Authority (CA) to issue digital certificates; a Registration Authority (RA) to collect and verify the basic information stored in the certificate; and a Directory (DIR) to distribute certificates to those who need them (Relying Parties).

6.1.4.1. Digital Certificates

Digital certificates are an electronic "proof of identity". They can be thought of as the digital equivalent of a passport, a driver's license (in the USA), or a national identity card (in most countries). A digital certificate uses cryptography to bind together (at least) a personal identity and the public key of a public/private key pair. Since the public/private key pair are used for digital signatures and key management, the person named in the certificate must have, and keep secret, the private key corresponding to the public key in the certificate.



6.1.4.2. Trusted Third Parties

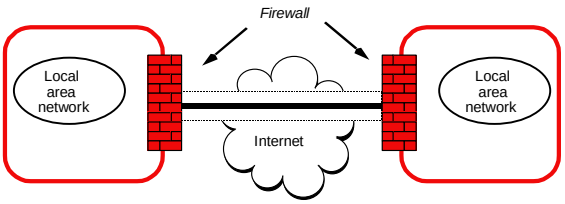
We frequently have need of notaries, arbiters, auditors, and advocates (often lawyers or agents) to support our pen and paper world transactions and keep our affairs working smoothly. Conducting business by electronic means will not reduce the need for support services from such "third party" agents. Electronic commerce will, however, change the nature of both the support agents themselves, and the protocols by which they operate.

In this relatively immature, and rapidly developing field there are already several fairly well understood third party services:

- Certification Authorities (CAs)
  A CA creates, for each of its clients, a cryptographically sealed certificate, attesting to the binding between the client's identity and the public key for the client's digital signature. Clearly the CA must be widely known, recognized and trusted.
- Directory Server Agents (DSAs) or Directories
  A DSA manages an electronic directory from which the recipient of a cryptographically signed message can retrieve the public keys needed to verify the origin and author of the message. DSAs are specified in the X.500 standard and accessed using the Directory Access Protocol (DAP) or the light-weight version of DAP, LDAP.
- Electronic Notaries
  An Electronic Notary can act as a guarantor or registry for electronic transactions or contracts between parties who do not entirely trust one another. The notary accomplishes its task by recording or cryptographically signing critical messages in the transaction.

6.1.5. Virtual Private Networks

A virtual private network (VPN) uses cryptography to provide a private channel between two or more closed, private networks, using an insecure public network as its carrier A VPN can be established, for example, by two firewalls, one protecting each of two local area networks (LANs), encrypting all traffic they send to each other over the Internet. The encryption effectively "punches a hole" through the Internet, hiding the content of all traffic between the two LANs, and establishing a virtual private network between the two. This very powerful technique for joining two security perimeters is currently being standardized and implemented as the IP Security or IPsec protocol.



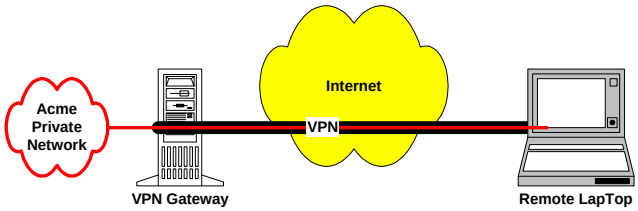
6.1.5.1. VPN Definitions

A Virtual Private Network is all of the following:

- A private communication path through a shared public network.
- A communication path providing confidentiality, integrity, and authenticity, over a shared, untrusted, public network.
- A clever trick to save lots of telcom $$.
- A violation of the 1st law of thermodynamics.
- Possibly too good to be true.

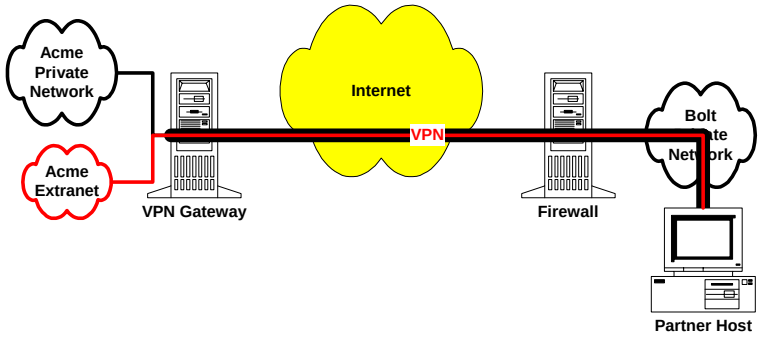
6.1.5.2. VPN Topologies

VPNs can be used as a remote dial-in replacement; a VPN connects roving user's laptop into the enterprise's private network, using the Internet instead of an expensive dial-up line.



VPNs can be used similarly as a leased line replacement to connect two geographically separated sites belonging to the same enterprise.

Another use of VPN technology is to provide "extranet" support of business partners. The VPN provides one or more hosts at the partner site with access to a controlled subset of the enterprise network. Here again the VPN can replace a dedicated line connecting the partner with the enterprise network. It also provides positive identification of the partner host computer, and ensures that no unauthorized systems can get access to the enterprise extranet. (This assumes that both parties utilize adequate security procedures).



- Host to Host
- Host or Site to Part of Site

6.1.5.3. VPN Protocols

The term VPN is used both for "tunneling" protocols and encryption protocols. Tunneling protocols allow one protocol to be encapsulated within, or "tunneled" through another; they provide transparent connections that might not otherwise be possible. Tunneling protocols do not necessarily provide confidentiality for the tunneled data. Encryption protocols, on the other hand, do provide data confidentiality; they may or may not use tunneling as well.

Tunneling protocols include:

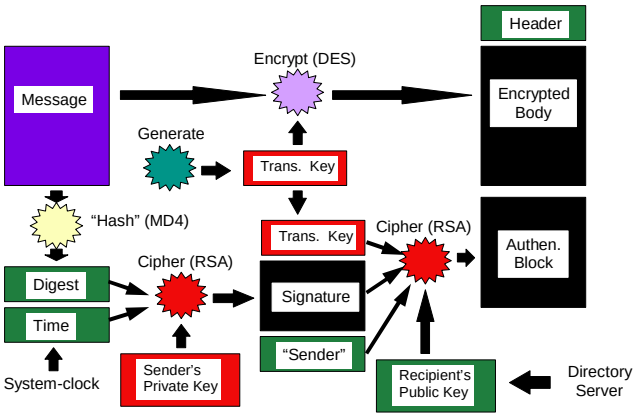
- IPSec tunnel
- L2F
- L2TP
- PPP

Encryption protocols include:

- PGP
- S/MIME
- SSH
- SSL
- Socks
- PPTP
- IPSec transport

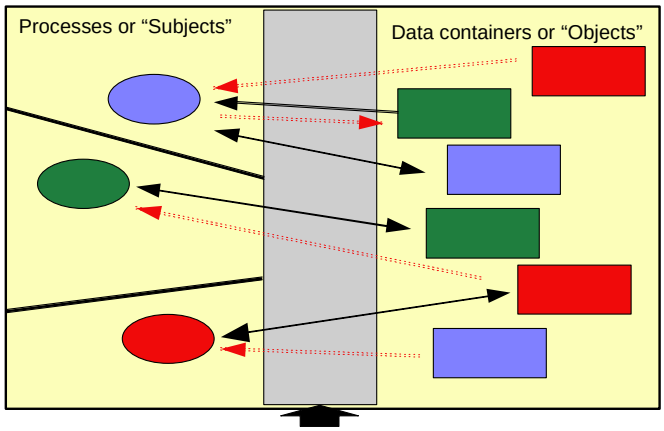
6.1.6. Secure E-Mail

The diagram on the right illustrates all of the cryptographic processing steps used to encrypt an e-mail message for confidentiality of its content, and to apply a digital signature that will verify the message integrity and testify to it authorship. In this diagram the rectangles represent data, the "star-bursts" represent cryptographic methods, and the arrows represent the flow of data. While this diagram is strictly illustrative, and does not correspond to any real e-mail encryption protocol, both Pretty Good Privacy (PGP) and Privacy Enhanced Mail (PEM) use techniques that are approximately like those shown.



6.1.7. Trusted-host Computer Systems

While perimeter security is an important tool for implementing an organization's security policy, it is necessary primarily because many of our host computer systems and all of our networks lack adequate security controls.



Reference Monitor:
Isolates each subject from all others
and controls all accesses by subjects to objects.

The Defense and Security establishments of the US and several European countries have, because of their special security needs, sponsored a great deal of research and some development toward the goal of designing and building operating systems capable of implementing very stringent security policies. These highly secure systems have come to be called "trusted computing bases" or TCBs.

This government sponsored TCB technology is beginning to appear in commercial products.

6.1.8. Intrusion Detection (ID)

Real-time monitoring for anomalous user behaviors or patterns of activity; unusual system or network loads or events; or attack-like actions.

Continuous checking for unchanged secure system configuration; "liveness" of systems and connections; integrity of system executable files; and integrity of logging processes and log files.

Generation of Alerts and Alarms, either console alarms if the system is attended; or automatic paging of system or security administrators.

6.1.8.1. Why ID is Hard

Intrusion detection is a classic "Hard Problem" in computer science. Intrusion detection presents a very large "search space", and must identify difficult to distinguish "patterns" in that space. There has been over ten years of research in intrusion detection approaches. Up until very recently, the best technology achieved low success rates on anomaly detection. Progress continues, but it is unlikely to be very rapid. The technical difficulties involved in intrusion detection are similar to those in several energy industry applications such as loose parts monitoring where the difficulty is establishing a trigger point that does not inhibit normal operation and minimizes false positive and negative indications.

The Internet and the wide adoption of distributed systems technology have made the problem more critical, and at the same time, they have made good solutions even harder to achieve. Some promising approaches include Ad Hoc "signature" definition with AI recognition engines.

6.2. Electronic Commerce Safeguards

Techniques very similar to those used for secure e-mail can be, and are being, used to protect Electronic Data Interchange (EDI) transactions. This approach is very attractive because EDI messages are effectively specially encoded e-mail messages. Encrypted EDI transactions could be carried over the Internet instead of over value added networks (VANs), reducing costs and increasing convenience and flexibility.

The huge growth in commercial use of the Internet, spurred by the convenience of HTTP-based world wide web (WWW) servers and browsers, has driven the rapid growth in electronic commerce. MasterCard and Visa have proposed a Secure Electronic Transaction (SET) specification defining transaction protocols for use between WWW Electronic Commerce Servers and Web browser clients. SET makes extensive use of cryptographic techniques.

Secure HTTP (S-HTTP) and Secure Sockets Layer (SSL) are two other protocols that provide protection for Web transactions. Both protocols provide similar functionality, however, their architecture and implementation are different.[6]

S-HTTP provides secure communication mechanisms between an HTTP client/server pair in order to enable spontaneous commercial transactions. The design intent is to provide a flexible protocol that supports multiple operation modes, key management mechanisms, trust models, cryptographic algorithms, and encapsulation formats through option negotiation between parties for each transaction.

Secure Sockets Layer (SSL) is an open protocol for securing data communications across computer networks. SSL uses RSA data security technology for authentication and provides a straightforward method for adding strong security to existing applications and network infrastructures. SSL is application protocol-independent and provides encryption, which creates a secured channel to prevent others from tapping into the parties in information exchanges and transactions; and message integrity, which ensures that messages cannot be altered en route.The privacy, integrity, and authentication of electronic transactions will rely heavily on cryptographic technology. The utility and success of these electronic transaction protocols will rely on cryptographic standards, key management standards, and third-party support. They will also depend on legal infrastructure or contractual agreements for their enforcement.

7. Basic Security Policies

7.1. Security Policies and Procedures

Information security begins with a security policy. The security policy defines the rules by which information should be managed. The security policy defines what information it controls, and it defines the users of that information. The security policy defines the information system users' responsibilities and the organization's expectations of those users.

Most organizations have IT security policies, but in many cases these policies are undocumented, relying on thoughtful users and "oral tradition". In many organizations, there is no security policy for non-IT systems. Defining and documenting a security policy should begin with a statement of organizational security goals; these high-level goals will then act as a guide and a reference point for the policies that follow. This should be followed by a gap analysis to determine what additional security policies beyond those developed for IT need to be applied to non-IT systems.

Drafting the security policy document should begin with a compilation of written policies related to security and a survey of informal policies applied by users by default. After the organizational "umbrella" policy has been written, reviewed and approved, the implementation of the policy can proceed.

Policy implementation will be accomplished partly by adding technical measures to existing systems, and partly through the definition of procedures people must follow.

[6] DOE Information Architecture Profile of Adopted Standards, http://www-it.hr.doe.gov/ standards.

7.1.1. Fundamental Policy Questions

There are three fundamental questions every organization needs to be able to answer in order to define a security policy:

- *What information* and to what level does the organization need to protect?
  This is defined in terms of organizational **information assets.**
- *Against whom* does the organization need to protect its information?
  This is defined in terms of the information **threats**.
- *How* will the organization protect its information?
  This is defined in terms of **protective measures** and **threat countermeasures**.

The answers to these questions will need to be tempered by careful consideration of the security versus convenience balance and the cost-benefit tradeoffs.

8. Risk Management

The processes of identifying, analyzing and assessing, mitigating, or transferring risk are generally characterized as Risk Management. [7]

8.1. Risk Assessment

Effective Risk Management requires the definition of the elements of risk through the execution of a Risk Assessment.

A Risk Assessment includes answering a few key questions[8]:

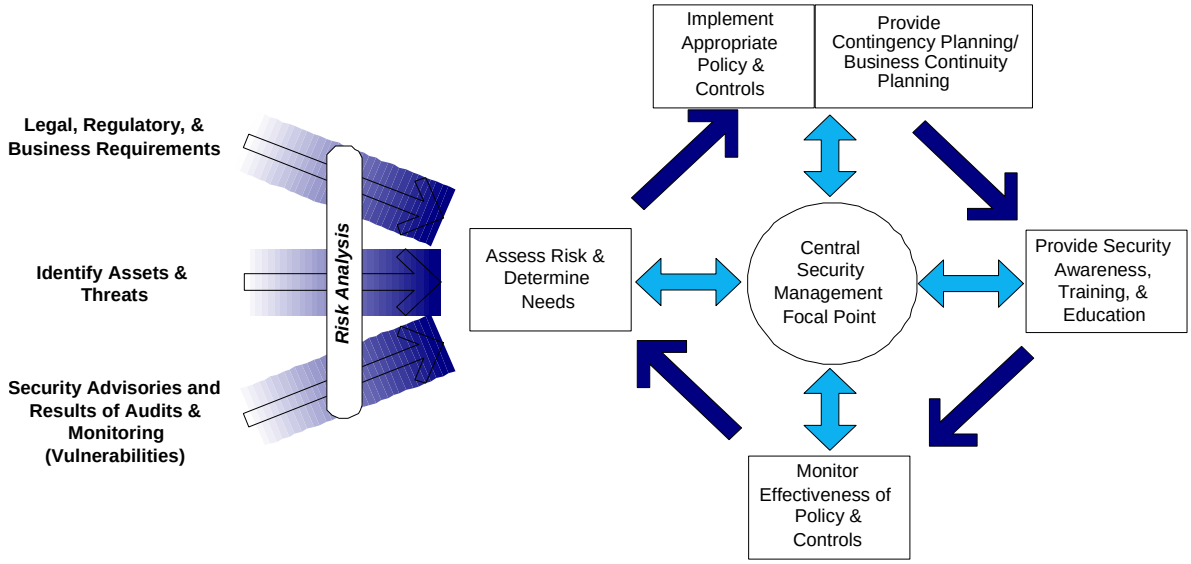
1. What could happen (threat event)?
2. If it happened, how bad could it be (threat impact)?
3. How often could it happen (threat frequency, annualized)?
4. How certain are the answers to the first three questions (recognition of uncertainty)?

8.2. Risk Management: Seeking Balance

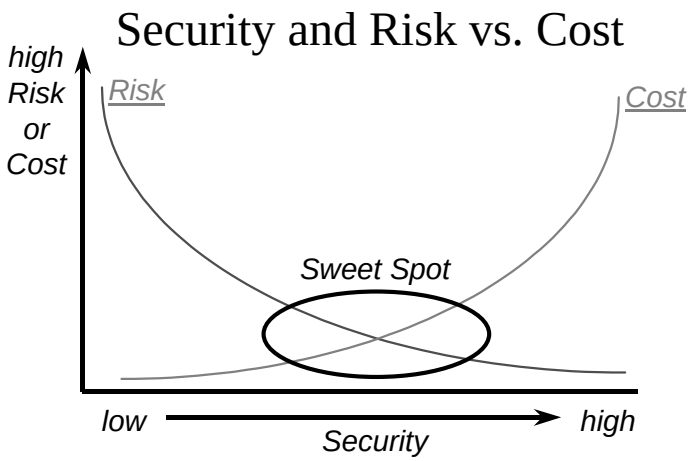
The following figure provides an overview of an Information Security Program Model that can be used to guide the Risk Management Process. This model is based on standards of good

[7] P. 426 Krause and Tipton, Handbook of Information Security Management, Auerbach, 1999.
[8] P. 426 Krause and Tipton, Handbook of Information Security Management, Auerbach, 1999.

practice[9], and is intended to guide activities in order to effectively manage the risks associated with the increasing evolution of automated and interconnected network environments.



The security policy is the foundation of the security program and the Risk Management process. The security policy may take into consideration the balance between the costs it is likely to impose and the benefit it seeks to ensure. Note that the costs to be considered include indirect costs such as extra work or inconvenience as well as direct financial costs. Initial security improvements are generally inexpensive for the improvement gained. As security improves, however, the cost of incremental improvements increases more and more rapidly (as illustrated). However, as security improves, risk is reduced, with the most dramatic reductions corresponding to those initial, inexpensive security improvements. Eventually risk approaches an irreducible, non-zero minimum. For most



[9] The source references used to establish Secure Computing Corporation's security program model are an accumulation of Secure Computing Corporation's Security Professional's experience and expertise and the following reference documents: The International Security Forum's (ISF) The Forums Standard of Good Practice – The Standards for Information Security, March 1998; British Standard 7799; United States General Accounting Office's (GAO) Executive Guide, Information Security Management: Learning From Leading Organizations, GAO/AIMD-98.68, May 1998, United States General Accounting Office's (GAO) Federal Information System Controls Audit Manual, Financial Statement Audits, GAO/AIMD-12.19.6, January 1999, International Federation of Accountants (IFAC), International Technology Guideline, Managing of Information Security, January 1998, Information Systems Audit and Control Foundation (ISACF), Control and Objectives for Information and Related Technology, (COBIT), April 1998

organizations, the most efficient level of security is that shown as the “sweet spot” in the figure, where risk reductions become slower, and security improvements start becoming more costly.

The security policy implementation measures must consider these trade-offs:

- Organizational (Business) Objectives
  - What does the organization need to achieve?
  - What benefits accrue from these achievements?
- Real Threats Against Objectives
  - What can happen to jeopardize achieving these objectives?
  - What is the likelihood of attacks against the organization?
  - Do adversaries have something to gain from an attack?
- Benefits of Security Measures
  - Do the security measures provide an effective deterrent to the threat?
  - Can the value of security be quantified for the organization?
  - Can the security measures help introduce new business opportunities?
- Costs of Security Measures
  - How much will it cost to build or buy and maintain appropriate security measures?
  - Can the organization still achieve its objectives with security measures in place?
  - What impact will security have on the operating flexibility of process control systems and operating effectiveness of plant staff?

The security policy should serve as a guide for employees and representatives into the correct actions necessary to protect the information and systems that are sensitive and critical to continued business operations. Specific areas generally covered in a security policy include:

- Acceptable use of information system resources
- Access control and password management
- Applications Security
- Contingency Planning, Business continuity planning and disaster recovery
- Clear roles and responsibilities.
- Configuration control and management
- External connectivity
- Information classification and handling guidance
- Network security
- Physical security
- Policy objectives
- Remote access
- Security awareness training

- Security incident identification and reporting
- System monitoring

9. Security Standards

9.1. Government

US Government agencies and organizations historically have played a critical part in security standards development and enforcement. Although many of these standards are not applicable beyond the Department of Defense and the US Government, their influence on non DoD organizations has been immense.

The following paragraphs contain brief descriptions of some of the better known government organizations/standards to provide an understanding of the role these played in commercial security development.

9.1.1. NIST

The National Institute of Standards and Technology (NIST) has a Computer Security Division that is chartered to improve information systems security by:

- Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;
- Developing standards, metrics, tests and validation programs:
  - to promote, measure, and validate security in systems and services
  - to educate consumers and
  - to establish minimum security requirements for Federal systems
- Developing guidance to increase secure IT planning, implementation, management and operation.

NIST also sponsors the Computer Security Resource Clearinghouse (CSRC) that is designed to collect and disseminate computer security information and resources to help users, systems administrators, managers, and security professionals better protect their data and systems. A primary goal of the CSRC is to raise awareness of all computer systems users -- from novice to expert -- about computer security. This is perhaps the most important way of improving information systems security. See http://csrc.nist.gov/ for additional information.

9.1.2. Common Criteria

In January 1996, the United States, United Kingdom, Germany, France, Canada, and the Netherlands released a jointly developed evaluation standard for a multi-national marketplace. This standard is known as the "Common Criteria for Information Technology Security Evaluation" (CCITSE) usually referred to as the "Common Criteria" (CC). See http://www.radium.ncsc.mil/tpep/library/ccitse/index.html for additional information.

The Common Criteria can be used for the following purposes:

Consumers

- To find requirements for security features that match their own risk assessment.
- To shop for products that have ratings with those features.
- To publish their security requirements so that vendors can design products that meet them.

Developers

- To select security requirements that they wish to include in their products.
- To design and build a product in a way that can prove to evaluators that the product meets requirements.
- To determine their responsibilities in supporting and evaluating their product.

Evaluators

- To judge whether or not a product meets its security requirements.
- Provide a yardstick against which evaluations can be performed.
- Provide input when forming specific evaluation methods.

9.1.3. TCSEC

The Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) was developed to serve a number of intended purposes:

- To provide a standard to manufacturers as to what security features to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements (with particular emphasis on preventing the disclosure of data) for sensitive applications.
- To provide DoD components with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information.
- To provide a basis for specifying security requirements in acquisition specifications.

9.1.4. DoD TAFIM

Technical Architecture Framework for Information Management (TAFIM) provide the DoD with a framework to manage technical architecture (TA) initiatives and is intended to achieve the following results:

- Use of common principles, assumptions, and terminology in DoD TAs.
- Definition of a single structure for DoD technical infrastructure components and how they are managed.
- Development of information systems in accordance with common principles to permit DoD-wide integration and interoperability.

TAFIM does not provide a specific architecture. It provides the services, standards, design concepts, components and configurations used to guide development of TAs meeting specific mission requirements. TAFIM is independent of mission-specific applications and their associated data. System architects and designers will use TAFIM as the basis for developing a common target architecture to which systems can migrate, evolve, and interoperate.

TAFIM introduces and promotes interoperability, portability, and scalability of DoD information systems. Over time, the number of compliant systems will increase, providing users with improved interoperability needed to achieve common functional objectives. To achieve portability, standard interfaces will be developed and implemented. Scalability will be developed in mission applications to accommodate functional flexibility.

9.2. Standards Organizations

The following organizations publish security standards that are of interest to the energy industry. The following paragraphs contain a brief description of each organization and a url to obtain more information.

ISO – reference http://www.iso.ch - The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from some 130 countries, one from each country. ISO is a non-governmental organization established in 1947. The mission of ISO is to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity. ISO's work results in international agreements which are published as International Standards.

ANSI – reference http://www.ansi.org/ - The American National Standards Institute (ANSI) has served in its capacity as administrator and coordinator of the United States private sector voluntary standardization system for more than 80 years. Founded in 1918 by five engineering societies and three government agencies, the Institute remains a private, nonprofit membership organization supported by a diverse constituency of private and public sector organizations.

IETF – reference http://www.ietf.org/home.html - The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). The IETF working groups are grouped into areas, and managed by Area Directors, or ADs. The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board, (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB.

9.3. Standards of Good Practice

Several membership organizations exist that publish Standards of Good Practice for their members. Two of the better known organizations are the Information Security Forum (ISF) and the Computer Security Institute (CSI).

Additional information on the ISF can be obtained at:

- http://www.securityforum.org/menu.htm

Additional information on CSI can be obtained at:

- http://www.gocsi.com/

Energy Industry Approach to Security

10. Security Remediation Process

10.1. Philosophy For Securing the Enterprise

Since the elimination of risk is impossible in the real world, IT managers must focus on risk reduction and risk management. Perfect security is an unattainable objective; managed risk is both desirable and can be achieved on a cost effective basis, Because security of enterprise information assets is a business issue, the enterprise decision makers — for example, the CEO, CFO, CIO, Board — must lead the effort. Because information is pervasive in the enterprise, everyone has a role to play. This means that everyone needs to understand the enterprise security policy and its implications for their day to day activities. Recognize that different processes may require different levels of security including some that require no security. Given this policy guidance, most employees will "do the right thing". Those who don't will need help or corrective action.

10.2. InfoSec Risk Reduction Process

The general approach to reducing information security risk, and thus reducing the consequent business risk, can be described by a simple four step process:

- Establish a security policy
  Identify information assets and decide how to handle them.
- Assess information system security
  Identify information assets, threats and vulnerabilities and evaluate current security posture.
- Plan security approach
  Evaluate risks based upon assessment, revise policy, develop security architecture and select countermeasures.
- Implement and manage system security
  Integrate and train, monitor, audit, correct behaviors and systems to manage risks to satisfy policy.

The security methodology described next elaborates this process.

10.3. Security Methodology

Improving the security of the enterprise need not be an extremely expensive or complex process. It does, however, require some rigor, and a well defined process is the best way to achieve it. A thorough security remediation methodology would have the following steps:

1. Identify critical information resources or assets.

2. Evaluate security risks and policy requirements regarding those information assets.

3. Assess and evaluate the enterprise's current security status or posture, based upon the policy requirements.

4. Rank and prioritize critical security deficiencies or "gaps" identified in the assessment.

5. Identify corrective measures — technical security safeguards or countermeasures, procedural changes, training, etc. — for each high-priority deficiency.

6. Develop a plan for implementing the corrective measures, in priority order, by applying the appropriate technical and non-technical solutions.

7. Implement the corrective measures.

8. Reassess the enterprise's security posture to measure progress and ensure effectiveness of corrective measures.

Because threats to information evolve continuously and an enterprise's operations change over time, it is a good idea to repeat the assessment process periodically to ensure continued protection of sensitive information and critical systems. When such periodic re-assessments reveal problems, the planning and implementation activities should be repeated as well.

11. Security "Tools"

11.1. Standards and Guidance

Standards of good security practice are beginning to appear. Additional information on these sources can be found in Section 9. Security Standards.

11.2. Policy

Drafting a good (clear, comprehensive, effective) information security policy is no harder than drafting any other policy with broad organizational impact. An excellent place to start is with a model policy for a specific industry, if one exists, or with examples from similar companies. There are also books and collections of policy statements ("policies") available, some in the public domain, and some for a modest fee.

11.3. Technology

There are technology-based "tools" to help with the assessment process, and to provide security safeguards.

Assessment tools include both network security assessment tools and host security configuration tools. Network assessment tools include free tools such as SATAN, and commercial tools such as Network Associate's CyberCop Security Scanner. Information on assessment tools is readily available on the WWW and in trade publications.

Technology safeguards have already been discussed extensively in the Security Overview. As a brief recapitulation, these safeguards include:

- Firewalls

- Authentication systems
- Virtual Private Networks (VPNs)
- Cryptography in general
- Public Key Infrastructure

The IT professionals charged with implementing security should always remember, however, that these technologies should be used to meet specific enterprise security needs. Implementing security technology for its own sake is not only a waste of resources, but it may lead to a false sense of security.

11.4. Operations

Sound day-to-day operational information security requires a solid security infrastructure. This security infrastructure is based upon a set of well defined organizational security processes and procedures, and appropriate management support.

The organizational requirements and functions needed to support security operations within the enterprise include organizational support for:

- Information Security Policy
- Information Security Audit and Control
- Security Feature Integration
  - Security Sensitivity Determination
  - Security Feature Integration
- Operational Security Management
- Incident Response Team

The key security management functions that must exist within an enterprise to support the security operations include:

- Key Non-functional Requirements
  - A strong commitment from management
  - A well defined site security philosophy
  - A well developed security awareness training program
  - Clearly defined security policies and procedures
  - An organizational structure with clear roles and relationships
  - A strong flow of information
  - The right people and the right tools to do the job
- Security Management Functional Requirements
  - Security Infrastructure Management Functions
  - Centralized Security Management Functions
    - Information Security Policy Formulation
    - Information Security Audit and Control
    - Information Security Policy Oversight

- Decentralized Organizational Functions
  - Security Feature Integration
  - Operational Security Management Function
- Incident Response Function

Effective Security Management requires that every user of enterprise information systems have the skills, disciplines and resources needed to use and maintain those systems and their data in a secure manner. Thus, all employees, and outsiders authorized to access the enterprise's systems and data, must know where they stand as regards their responsibilities for information security.

Annex: Resources

12. Acronyms and Abbreviations

ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FBCA QA	Federal Bridge Certification Authority Operational Aut
FED-STD	Federal Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
GITSB	Government Information Technology Services Board
GPEA	Government Paperwork Elimination Act of 1998
IETF	Internet Engineering Task Force
ISO	International Standards Organization
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union — Telecommunications Sector
ITU-TSS	International Telecommunications Union — Telecommunications System Sector
MOA	Memorandum of Agreement (as used in the context of this CP, between an Agency and the FPKIPA allowing interoperation between the FBCA and Agency Principal CA)
NIST	National Institute of Standards and Technology
NSA	National Security Agency

OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure *X.509*
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm, Version 1
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

13. Definitions

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS40091
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Applicant	The subscriber is sometimes also called an “applicant” after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32)

Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the FPKIPA or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Authority Revocation List (ARL)	A list of revoked CA certificates. An *ARL* is a CRL for CA cross-certificates.
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and *(5)* is digitally signed by the certification authority issuing it. [ABADSG]. As used in this Policy, the term "Certificate" refers to certificates that expressly reference the OID of this policy in the "Certificate Policies" field of an *X.509* v.3 certificate.

Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and ARLs or CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certification Authority Software	The cryptographic software required to manage the certificates of subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificatebased security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Policy, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a relying party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine: (1) whether the transformation was created using the key that corresponds to the signer's key; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue."

Employee	Any person employed by an Agency as defined above.
Encrypted Network	A network that is protected from outside access by NSA approved high grade (Type I) cryptography. Examples arc SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers who are not authorized to issue certificates.
Federal Bridge Certification Authority FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer to peer interoperability among Agency Principal Certification Authorities.
FBCA Operational Authority (FBCA OA)	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]

Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communication.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.

Memorandum of Agreement (MOA)	Agreement between the FPKIPA and an Agency allowing interoperability between the Agency Principal CA and the FBCA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).

Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA.
Principal CA	The Principal CA is an Agency CAs that the Agency has selected to interoperate with the FBCA. An Agency may designate more than one Principal CA.
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law and agency policy.
Private Key	(1) The signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(I) The signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Rekey (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system. [NS4009]
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in providing subscriber identification during the registration process. Trusted agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure, authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a “trust anchor”.
	Computer hardware, software and procedures that: (1) are reasonably secure from

Trustworthy System	intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

14. Books on Security

- ***Computer Security Basics***,. Deborah Russell & G. T. Gangemi Sr. O'Reilly & Associates: 1991
- ***Web Security & Commerce***. Simson Garfinkel with Gene Spafford. O'Reilly & Associates: 1997
- ***Internet Security for Business.*** Terry Bernstein (editor). John Wiley & Sons: June 1996
- ***Frontiers of Electronic Commerce***, Ravi Kalakota & Andrew B. Whinston. Addison-Wesley: 1996.
- ***Computer Crime: A Crimefighter's Handbook***. Icove, Seger & VonStorch. O'Reilly & Associates: 1995
- ***Internet Cryptography.*** Richard E. Smith. Addison-Wesley: August 1997
- Web Security: A Step-by-Step Reference Guide. Lincoln D. Stein, Addision-Wesley: 1998

15. General Security Web Sites

Computer and network security

- Security fixes announced by the Computer Emergency Response Team (CERT®): "http://www.cert.org/"

- Other Sources of Security Information from CERT: "http://www.cert.org/other_sources/other_teams.html"
- Hackers 2600 Magazine: http:// www.2600.com/title_index.html
- Security alerts by the Computer Incident Advisory Capability (CIAC): http://www.alw.nih.gov/Security/CIAC-Notes.html
- AusCERT - Australian CERT: "http://www.auscert.org.au/"
- SANS: "http://www.sans.org/"

16. Electronic Commerce Sites

Electronic Commerce

- "EDI Meets the Internet", Walt Houser et al. Available at http://www.va.gov/publ/standard/edifaq/index.htm
- Phillip Hallam-Baker's payments roadmap: http://www.w3.org/payments/roadmap.html

17. "Dark side" web sites

Keeping track of incidents, tools & hacks.

- S e c u r i t y f o c u s: "http://www.securityfocus.com/"
- SecurityPortal.com: "http://www.securityportal.com/"
- ISS X-Force: "http://xforce.iss.net/"
- ATTRITION: "http://www.attrition.org/"
- AntiOnline - Computer Security - Hacking & Hackers: "http://www.antionline.com/"
- HNN - H a c k e r N e w s N e t w o r k: "http://www.hackernews.com/index.html"
- (and lots more . . .)

18. Personal favorites

Some theory, some practice, some . . .

- Bert-Jaap Koops maintains the "Crypto Law Survey": http://cwis.kub.nl/%7Efrw/people/koops/lawsurvy.htm
- Dan Farmer (author of COPS and SATAN) has an interesting security page: http://www.trouble.org/security
- Dan Farmer's 1996 survey is still worth reading: http://www.trouble.org/survey
- Wietse Venema has a set of interesting security tools: ftp://ftp.win.tue.nl/pub/security/index.html

- Ross Anderson on Privacy, Cryptography and Security: http://www.cl.cam.ac.uk/users/rja14/
- Princeton Secure Internet Programming team (esp. for Java): http://www.cs.princeton.edu/sip/

19. Security mail lists

Security E-mail Lists for Technologists:

- CERT-advisory-request@cert.org: The Computer Emergency Response Team (CERT) issues advisories for security holes.
- CERT-tools-request@cert.org: CERT's tools mailing list keeps subscribers up-to-date on security tool news.
- ntbugtraq@listserv.ntbugtraq.com: Moderated list of NT bugs
- firewall-wizards@nfr.net: The Firewall Wizards Mailing List moderated by Marcus J. Ranum.
- cryptography@c2.net: Cryptography mailing list
- microsoft_security@announce.microsoft.com: to keep track of Microsoft security bug announcements